UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,785	11/22/2000	Cary A. Jardin	042390.P8899	3950

7590 05/24/2006

Crystal D Sayles
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard
7th Floor
Los Angeles, CA 90025

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/721,785	JARDIN ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-12,15,16,19 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-12,15,16,19 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-3, 6-12, 15-16, and 19-20 are pending. Any objections or rejections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

Response to Amendment and Arguments

Applicant's amendments have been fully considered. Applicant's arguments have also been fully considered, but are moot in view of new grounds of rejections presented below in response to the amendments.

Information Disclosure Statement

Documents listed in the IDS submitted on 4/27/2006 have been considered.

Claim Objections

Claims 19 and 20 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claims 12 and 16 are the parent claims of claims 19 and 20 respectively. The parent claims already established that the link reverts to the HTTP non-secured protocol when the detected failures or intrusions have been corrected. Claims 19 and 20 seem to merely repeat this limitation with the added information that the determination was done by a network manager. However, one skilled should appreciate that in the parent

claims, the determination must have been done by a network manager. Thus, it does not appear that claims 19 and 20 really further limit the parent claims since the added information is already inherent to the parent claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 7, 12, 15-16, and 19-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 7 recites "the secured protocol" in line 3, which lacks antecedent basis. It is unclear if the secured protocol being referred to in claim 7 is HTTP-S or another type of secure protocol.
2. Claim 12 recites directing the link to use an HTTP-S secured protocol and directing the link to revert to an HTTP non-secured protocol. HTTP-S is itself a protocol which is secure, so it is unclear how one can use a secured protocol of a secured protocol. Likewise, HTTP is itself an unsecured protocol. It is unclear how one can use a non-secured protocol of a non-secured protocol. A similar problem exists for claims 16, 19, and 20.
3. Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 6-12, 15-16, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US 6,473,863) in view of applicant's admittance of prior art.

Claim 1:

Genty discloses:

1. A computer (col 3, lines 14-26).
2. A network interface device to provide the computer with access to the network (col 3, lines 14-26).
3. A bus monitor to monitor a first link between the network interface device and the computer, where the bus monitor reports detected failures or intrusions (col 5, lines 48-52).
4. A security switch to switch the first link from a first mode to a second mode when a report of the detected failures or intrusions is received from the bus monitor (col 5, lines 48-59 and col 6, lines 1-6).

Note that Genty discloses that a typical end-to-end path typically contains several machines such as a gateway, firewall, router, or even the Internet (col 1, lines 44-56).

As used in her invention, a node is a standalone computer or a computer along with a gateway or several gateways and a router (col 3, lines 14-26). One skilled should appreciate that gateways and routers are network interface devices which provide a computer in a LAN access to a network outside the LAN. Figure 1 shows a system where Genty's invention is used. Genty discloses that items 110, 112, and 114 are all nodes on the Internet 116 (col 3, lines 47-49). Figure 1 shows that one end of a data path/first link is Intranet 110 and the other end is Remote Access device 114 or Associate Intranet 112. One skilled should appreciate from Genty disclosing that an end-to-end path contains several machines, i.e. network interface devices, that when Genty's invention monitors a VPN tunnel to detect a security breach or failure, Genty is monitoring the links between the node 110 and items 114 and 112, which contains a first link between a network interface device and a computer since a node comprises a computer and network devices, i.e. gateways, routers, and the Internet.

Genty does not disclose the first mode is a non-secured mode using an HTTP protocol and the second mode is a secured mode using an HTTP-S protocol. However, HTTP and HTTP-S were well known web protocols at the time applicant's invention was made. This was also admitted by applicant (specification, page 2). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Genty's invention such that the first mode utilized the non-secured HTTP protocol and the second mode utilized the secured HTTP-S protocol because HTTP and HTTP-S were the standard web protocols used to transfer web pages at the time applicant's invention was made. One skilled would have been motivated to utilize HTTP

when there was not a security breach detected and utilize HTTP-S when a breach was detected because HTTP is faster than HTTP-S, while HTTP-S is more secure than HTTP. VPN already offers some security, therefore if the link provided via the VPN tunnel was secure, one skilled would most likely want to use the faster protocol while if there is increased danger of a security breach, one skilled would most likely want to increase security by utilizing HTTP-S since it had already been proven that the security provided via VPN alone may not be enough to keep the data transferred via the first link secure.

The examiner interpreted the first link as the data path used by the computer to send data. In Genty's invention, the first link starts out as the first VPN tunnel and later becomes the second VPN tunnel when a security breach or failure is detected. This switch from the first tunnel to the second tunnel is interpreted as the switch from a first mode to a second mode.

Claim 2:

Genty further discloses the computer is a server (col 3, lines 40-41). Remote access machine 114 accesses intranet 110—this implies a client/server relationship, where the computer located in intranet 110 is the server and machine 114 is the client.

Claim 3:

Genty implicitly discloses the network operates in the secured mode using the HTTP-S protocol (Fig 1, item 116). One skilled should appreciate that computers on the Internet operates in the secured mode using the HTTP-S protocol.

Claim 6:

Genty further discloses a controller that receives the report from the bus monitor and sends a control signal to the network interface device, the security switch, and the computer (col 5, lines 48-59 and col 6, lines 1-5).

Claim 7:

Genty further discloses an encryption element in the computer, where the encryption element converts data placed on the first link using the secured protocol when the control signal is received from the controller (col 4, lines 6-9 and col 7, lines 3-11).

Claim 8:

Genty discloses:

1. An interface device to provide the server with access to a network (col 3, lines 14-26).
2. A controller to monitor a link between the interface device and the server, where the controller switches the link from a first protocol to a second protocol when failures or intrusions are detected on the secured link (col 5, lines 48-52 and col 6, lines 1-6).

Genty does not disclose the first protocol is a non-secured protocol using an HTTP protocol and the second protocol is a secured protocol using an HTTP-S protocol. However, as noted in claim 1, HTTP and HTTP-S were admitted by applicant as being known protocols at the time applicant's invention was made and it would have been obvious to one skilled to modify Genty's invention such that the first protocol was non-

secured protocol using an HTTP protocol and the second protocol is a secured protocol using an HTTP-S protocol. One skilled would have been motivated to do so for the same reasons given in claim 1.

Claim 9:

Genty further discloses wherein the network is the Internet (Fig 1, item 116).

Claim 10:

Genty further discloses wherein the controller sends a control signal to the server when failures or intrusions are detected on the link (col 5, lines 48-59 and col 6, lines 1-6).

Claim 11:

Genty further discloses an encryption element in the server (col 7, lines 3-11). One skilled should further appreciate that in Genty's modified invention, because the secured protocol used is HTTP-S, the encryption element converts the data placed on the link by the server using the secured protocol (HTTP-S) when the control signal is received from the controller since the control signal would signal a change from HTTP to HTTP-S.

Claim 12:

The limitations in claim 12 of monitoring a link between a network device and a computer and first directing the link to use an HTTP-S secured protocol when failures or intrusions are detected on the link are limitations describing the use of the system of claim 1 and are rejected for substantially the same reasons claim 1 is rejected.

Genty does not disclose second directing the link to revert to an HTTP non-secured protocol when the detected failures or intrusions have been corrected. However, as discussed previously, HTTP is substantially faster than HTTP-S since HTTP-S is basically HTTP over SSL (it is actually on average around 30% faster). Further, it was well known at the time applicant's invention was made to revert to the original operating mode once an error has been corrected. For instance, a network system which has a broken piece of equipment (such as a router) may continue to operate by bypassing the broken equipment, but once the equipment has been repaired, it is standard to start using the repaired equipment again, i.e. revert back to the original configuration. Otherwise, it would be a waste of time to repair the equipment and not use it.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Genty's invention such that it reverted back to using HTTP when the detected failures or intrusion has been corrected. One skilled would have been motivated to do so because with the failure or intrusion corrected, it would be a better use of system resources to utilize the faster transmission protocol since security is no longer as big a concern.

Claim 15:

Genty further discloses the computer is a server (col 3, lines 40-41). Remote access machine 114 accesses intranet 110—this implies a client/server relationship, where the computer located in intranet 110 is the server and machine 114 is the client.

Claim 16:

Claim 16 recites limitations substantially similar to claim 12 and is rejected for the same reasons. The difference between the two claims is that claim 12 is a method claim and claim 16 is directed towards an apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to implement the method of claim 12.

Claims 19 and 20:

As per claims 19 and 20, the claims are directed towards reverting to the link to HTTP non-secured protocol when the detected failures or intrusions have been corrected and the determination of when it was corrected was done by a network manager. It was discussed in claim 12 how it would have been obvious to revert the link to HTTP non-secured protocol when the detected failures or intrusions have been corrected. One skilled should appreciate that the determination would be done via a network manager.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

PP